

ABSTRACT

The present invention provides a multicast communication system having a multicast server and a plurality of clients belonging to a multicast group. The multicast server transmits data encrypted by using a first encryption key to the clients by multicasting, and transmits the result of encrypting the first encryption key by using a second encryption key by unicasting to a client subscribed to a data distribution service, among the plurality of clients. The client subscribed to the data distribution service receives the encrypted data and the result. The client decrypts the result to obtain the first encryption key and decrypts the encrypted data using the first encryption key.